



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/997,232	11/28/2001	Robert R. Oberle	033279-006	2534
7590	03/08/2006		EXAMINER	
Sheldon R. Meyer FLIESLER DUBB MEYER & LOVEJOY LLP Four Embarcadero Center Fourth Floor San Francisco, CA 94111-4156			MIZAN, SHAHIN	
			ART UNIT	PAPER NUMBER
			2132	
DATE MAILED: 03/08/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/997,232	OBERLE ET AL.
	Examiner	Art Unit
	Shahin Mizan	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 11 January 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-30 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-30 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 19 February 2002 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendments/arguments with respect to amended claims 1-30 filed January 11, 2006 have been fully considered (MPEP 714.04; 37 CFR 1.111) but they are not persuasive. Amendments to the specification have been accepted.

Response to Arguments

2. Applicant's arguments with respect to claims 1-30 have been considered but are not persuasive.

With regards to Applicant's argument that the use of password input from a user interface at the RFID unit is not shown or suggested in the Nerlikar reference, Examiner respectfully disagrees (*note Fig. 1 – the user ID badge is authenticated by the RFID reader. The authentication can be achieved by providing a password via the input/output data port [column 7, line 15]. Authentication implies password authentication, biometrics authentication or any other appropriate means*)

With regards to Applicant's argument that Nerlikar describes an input/output data means at the badge, but this input/output data means isn't used to receive a password for a user and that the input/output data means appears to be associated with a encryption or data handling for the Personal Computer Memory Card Interface (PCMCG) standard, Examiner respectfully disagrees (*note column 7, line 15 - the input/output data port associated with a type II PCMCIA card can be used for interfacing a keypad via which password or other authentication related information can be provided*).

Art Unit: 2132

With regards to Applicant's argument that Nerlikar does not disclose, suggest or give a motivation for having a user input a password at the RFID unit, which is then sent using the RFID signals and that the reference doesn't disclose the use of user interface that can receive a user password input at the RFID unit, Examiner respectfully disagrees (*note Fig. 1 – the authentication functionality shown between the user ID badge and the RFID reader incorporates the password feature. The password can be inputted via the described I/O data port. Nerlikar does not forbid the use of password, but rather points out a shortcoming associated with such an approach and provides robust alternatives.*).

With regards to Applicant's argument that claims 2-15, 17-24, and 26-30 are dependent upon of the above discussed independent claims and for that reason and because of the additional limitation of these claims, these claims are believed to be allowable, Examiner respectfully disagrees (*note the explanation of the independent claims above*).

With regards to Applicant's argument that Nerlikar does not disclose, suggest or give a motivation for using a keypad as the user interface at the RFID unit, Examiner respectfully disagrees (*the keypad feature associated with the dependent claim 15, 24, and 30 can be achieved via the PCMCIA type II data port described in the specification*).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Nerlikar (US Patent No. 5,629,981).

As per independent claim 1, Nerlikar teaches a system comprising:

an RF ID unit (*note Fig. 3A and Fig. 3B - RF ID unit is the badge*); and

an RF ID reader, wherein the RF ID unit is adapted to transmit a stored ID to the RF ID reader, the RF ID unit adapted to encrypt a password input from a user interface to form an encrypted message, the RF ID unit adapted to transmit the encrypted message to the RF ID reader, the RF ID reader adapted to use the ID to obtain a key to decrypt the encrypted message with the key and to authenticate the RF ID unit (*note Fig. 3C and Fig. 6 – shows the RF ID reader; also note column 6, line 11; also note column 7, lines 16 - 22 - the transponder is equipped with cryptographic capability; also note Fig. 1*).

As per claim 2, which is dependent on claim 1, Nerlikar teaches the system of claim 1, wherein the user interface is on the RF ID unit (*note column 7, line 15 – the input/output port allows for user interface which may be implemented on the transponder*).

As per claim 3, which is dependent on claim 1, Nerlikar teaches the system of claim 1, wherein user interface is on another device that is attachable to the RF ID unit (*note column 7, line 15 – the input/output port allows for user interface which may be implemented as a separate device by extending the I/O port*).

As per claim 4, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the RF ID reader transmits additional data to the RF ID unit, the transmitted message including an encrypted password and the additional information

(note column 9, lines 1 - 40 - describes information sent to the transponder by the RF ID reader; also note column 4, lines 1 - 14).

As per claim 5, which is dependent on claim 4, Nerlikar teaches the system of claim 4 wherein the additional information is a timestamp (*note column 8, line 11 - date, time, and location are additional information; also note Fig. 4*).

As per claim 6, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the RF ID reader and the RF ID unit use the same key (*note column 11, lines 43 - 45 – any currently available cryptography mechanism is useable which may include same key configuration; also note Fig. 1*).

As per claim 7, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the RF ID reader and the RF ID unit use a different key (*note column 11, lines 43 - 45 – any currently available cryptography mechanism is useable which may include different key configuration; also note Fig. 1*).

As per claim 8, which is dependent on claim 7, Nerlikar teaches the system of claim 7 wherein the RF ID reader and the RF ID unit encrypt and decrypt using a public/private encryption algorithm (*note column 11, lines 43 - 45 – any currently available cryptography mechanism is useable which may include public/private encryption algorithm; also note Fig. 1*).

As per claim 9, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the ID is used to look up key and password (*note column 4, lines 1 - 14 – the host computer performs these functions*).

As per claim 10, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the RF reader is associated with an external network, the RF ID reader

sending the ID to the external network to obtain the key, and the RF ID reader sending the encrypted message to the external network (*note column 4, lines 1 - 14 – the host computer performs these functions; also note Fig. 1 and Fig. 2*).

As per claim 11, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the system is used to authenticate a user (*note column 7, lines 61 - 64 – identifying an individual is part of the invention*).

As per claim 12, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the system is used to provide a secure passage of a user within a building (*note Fig. 1 – hardware and software exists for authentication; also note column 7, lines 61 - 64 – identifying an individual is part of the invention; also note column 13, lines 18 - 22; also note column 11, lines 47 - 59 – describes an example that may be used to accomplish secure passage function*).

As per claim 13, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the system is used for authentication (*note Fig. 1 – hardware and software exists for authentication; also note column 7, lines 61 - 64 – identifying an individual is part of the invention; also note column 13, lines 18 - 22; also note column 11, lines 47 - 59 – describes an example that can be used to accomplish this function*).

As per claim 14, which is dependent on claim 13, Nerlikar teaches the system of claim 13 wherein the system is used for commercial transaction authentication (*note column 3, line 64 – the system is transaction based; also note column 12, lines 43 - 53 – commercial financial transaction functionality is described*).

As per claim 15, which is dependent on claim 1, Nerlikar teaches the system of claim 1 wherein the user interface is a keypad (*note column 7, line 15 – the input/output port allows for user interface which may be implemented as a keypad*).

As per independent claim 16, Nerlikar teaches a method comprising:

transmitting an ID from an RF ID unit to an RF-ID reader (*note column 9, lines 1 - 40 - the transponder sends RF ID when interrogated*);

receiving a password from a user interface (*note column 7, line 15 – the input/output port allows for user interface which may be implemented as a keypad for entering user information such as a password; also note column 9, last line*);

encrypting the password to form an encrypted message (*note column 7, lines 16 - 21 – decryption/encryption mechanism is described; also note column 9, lines 1 - 40 - the transponder sends encrypted message when interrogated; also note column 12, line 47 – biological authentication is allowed*); and

transmitting the encrypted message from the RF ID unit to an RF-ID reader (*note column 9, lines 1 - 40 - the transponder sends encrypted message when interrogated; also note Fig. 1 and Fig. 2*).

As per claim 17, which is dependent on claim 16, Nerlikar teaches the method of claim 16 wherein the user interface is on the RF ID card (*note column 7, line 15 – the input/output port allows for user interface which could be implemented on the transponder*).

As per claim 18, which is dependent on claim 16, Nerlikar teaches the method of claim 16 wherein the user interface is on another device attachable to the RF ID card (*note column 7, line 15 – the input/output port allows for user interface which may be implemented as a separate device by extending the I/O port*).

As per claim 19, which is dependent on claim 16, Nerlikar teaches the method of claim 16 wherein additional data is provided from the RF ID reader to the RF ID unit, the RF ID unit encrypting the password along with the additional data to form the

encrypted message (*note column 9, lines 1 - 40 - describes information sent to the transponder by the RF ID reader; also note column 4, lines 1 - 14*).

As per claim 20, which is dependent on claim 16, Nerlikar teaches the method of claim 16 wherein the additional data is a time-stamp (*note column 8, line 11 - date, time, and location are additional information; also note Fig. 4*).

As per claim 21, which is dependent on claim 16, Nerlikar teaches the method of claim 16, further comprising decrypting the encrypted message (*note Fig. 1 – the crypto module perform this function; also note column 7, lines 16 - 21 – decryption/encryption mechanism is described*).

As per claim 22, which is dependent on claim 16, Nerlikar teaches the method of claim 16 wherein the encryption method is a public/private encryption method (*note column 11, lines 43 - 45 – any currently available encryption/decryption method is useable; also note Fig. 1*).

As per claim 23, which is dependent on claim 16, Nerlikar teaches the method of claim 16 wherein the encryption is a hidden key encryption system (*note column 11, lines 43 - 45 – any currently available cryptography is useable which may include hidden key encryption; also note Fig. 1*).

As per claim 24, which is dependent on claim 16, Nerlikar teaches the method of claim 16 wherein the user interface is a keypad (*note column 7, line 15 – the input/output port allows for user interface which may be implemented as a keypad*).

As per independent claim 25, Nerlikar teaches an RF ID unit with a user interface (*note column 7, line 15 – the input/output port allows for user interface*), the RF ID unit adapted to transmit a stored ID to a RF ID reader (*note column 9, lines 1 - 40 - the transponder sends RF ID*

when interrogated), the RF ID unit adapted to encrypt a password input from the user interface to form an encrypted message (note column 7, lines 16 - 21 – decryption/encryption mechanism is described; also note column 9, lines 1 - 40 - the transponder sends encrypted message when interrogated; also note column 12, line 47 – biological authentication is allowed), the RF ID unit adapted to transmit the encrypted message to a RF ID reader (note column 9, lines 1 - 40 - the transponder sends encrypted message when interrogated; also note Fig. 1 and Fig. 2).

As per claim 26, which is dependent on claim 25, Nerlikar teaches the RF ID unit of claim 25 wherein the RF ID unit receives additional data from the RF ID reader, the additional data being encrypted along with the password to form the encrypted message (*note column 9, lines 1 - 40 - describes information sent to the transponder by the RF ID reader; also note column 4, lines 1 - 14; also note column 9, lines 1 - 40*).

As per claim 27, which is dependent on claim 26, Nerlikar teaches the RF ID unit of claim 26 wherein the additional data is a time-stamp (*note column 8, line 11 - date, time, and location are additional information; also note Fig. 4*).

As per claim 28, which is dependent on claim 25, Nerlikar teaches the RF ID unit of claim 25 wherein the encryption is a public-key/private-key encryption system (*note column 11, lines 43 - 45 – any currently available encryption/decryption method is useable; also note Fig. 1*).

As per claim 29, which is dependent on claim 25, Nerlikar teaches the system of claim 25 wherein the encryption is a hidden key encryption system (*note column 11, lines 43 - 45 – any currently available cryptography is useable which may include hidden key encryption; also note Fig. 1*).

As per claim 30, which is dependent on claim 25, Nerlikar teaches the system of claim 25 wherein the user interface is a keypad (*note column 7, line 15 – the input/output port allows for user interface which may be implemented as a keypad*).

Conclusion

6. **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Inquiries

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shahin Mizan whose telephone number is 571-272-0687 and whose fax number is 571-273-0687. The examiner can normally be reached on M-F 8:30 a.m. - 5:00 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shahin Mizan
Examiner
Art Unit 2132

SM
SM

Gilberto Barron Jr.
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100